

The Quantum Car

Robert Malaney*

Abstract—I explore the use of quantum information as a security enabler for the future driverless vehicle. Specifically, I investigate the role combined classical and quantum information can have on the most important characteristic of the driverless vehicle paradigm - the vehicle location. By using information-theoretic verification frameworks, coupled with emerging quantum-based location-verification procedures, I show how vehicle positions can be authenticated with a probability of error simply not attainable in classical-only networks. I also discuss how other quantum applications can be seamlessly encapsulated within the same vehicular communication infrastructure required for location verification. The two technology enablers required for the driverless quantum vehicle are an increase in current quantum memory timescales (likely) and wide-scale deployment of classical vehicular communication infrastructure (underway). I argue the enhanced safety features delivered by the ‘Quantum Car’ mean its eventual deployment is inevitable.

Introduction - In next-generation wireless networks, location information will be elevated to an almost pivotal role. A clear example of this is in the emerging vehicular network paradigm, e.g., [1, 2]. In this paradigm, vehicles will communicate various attributes on themselves (e.g. speed, direction, location) every 100 milliseconds. Such information will be combined with information gathered from on-board sensors such as laser systems, optical-recognition systems, and spatial-map processors, so as to deliver the driverless-car paradigm, e.g. [3]. Great strides are already being made in this endeavor, and many would argue that the (classical) driverless vehicle 1.0 has already arrived. One aim of this letter is to encourage consideration of the enhanced benefits offered by the driverless vehicle 2.0 - the quantum version.

Clearly, the accuracy and verification of the location information in vehicular networks will be a mission-critical requirement. However, upon trying to unconditionally verify the location of a vehicle solely within the classical realm we are immediately confronted by a noteworthy problem - it is impossible. Classical information can be copied, thus rendering any location verification system solely based on it attackable from a well-resourced adversary, e.g. [4, 5]. A potential solution to this is quantum location verification (QLV). As the name implies, QLV in essence adds quantum information into the location verification process. Such information, unlike its classical counterpart, cannot in general be copied exactly - the no cloning theorem [6]. This theorem leads to QLV when it is coupled to another law of physics - the no-signalling principle of relativity.

The notion of QLV first appeared in the scientific literature in 2010, as a means of securing real-time classical commu-

nications to a *unique* spatial position [7].¹ Since then many works related to QLV have appeared in the literature, e.g. [8–15], largely focusing on information-theoretic security issues under different conditions. As I discuss more later, it is widely accepted that under known attacks, QLV is *effectively* secure. It is the main purpose of this letter to investigate the performance of QLV under the two most feasible attacks, showing how quickly it can overcome such attacks to any required accuracy. I also highlight how other quantum technologies using the same QLV infrastructure lead to a much-enhanced, and effectively *unhackable*, vehicular network.

QLV in Vehicular Networks - Within our system a reference station (RS) is defined as any communicable device within the vehicular network infrastructure whose location has already been authenticated. The prover vehicle (PV) in the system is a vehicle which is yet to be authenticated (i.e. its claimed location is yet to be verified). I will assume that most (if not all) of the quantum information to be used in the QLV protocol is pre-stored in the PV’s on-board quantum memory. This information could have been delivered to the PV through an optical communication network (for example) when the PV was last hooked into its ‘electric-quantum’ charging station.

To help keep our adversary (Eve) on her toes, I will assume that the stored quantum states are non-orthogonal and take any allowable (possibly hidden) form, e.g. continuous variable (CV) states, qubits, qudits, hybrids, etc. I allow for some states being entangled (possibly with states at multiple RSs). I will assume that coded signals sent from the RSs to the PV (instructing the PV in each round as to which operations to undertake on which quantum states) are wireless signals traveling at light-speed - I refer to these signals as the verification information (VI). All VI (in a single round of the protocol) is obtained by the PV at the same instant. I will assume that the VI is encoded across a subset of RSs (randomly selected at each round), and all communications between RSs are secure (e.g via quantum keys). The actual number of RSs encoding the VI can also form part of the coded VI (i.e. a null signal from an RS can form part of the code). Coded VI received could imply instructions related to subsequent VI arriving ϵ_t time later. The number of bits of information encoded in the VI signal (for at least some rounds) can be *a priori* unknown. In general, the output of the PV upon receipt of the VI will be classical and/or quantum signals sent to at least three RSs. To pass a verification test, the time taken to receive this output must be bounded by the round-trip time for the RS-PV communications, plus the legitimate-receiver

¹Two months after [7] another proposal on QLV appeared in the literature [9]. Three months after [9], a 2006 patent [16] on ‘tagging systems’ for line-of-sight objects, based on entanglement, was first brought to my attention [17]. To the best of my knowledge, the patent [16] first introduced the application of quantum information to object location verification.

*Robert Malaney is with the School of Electrical Engineering and Telecommunications at the University of New South Wales, Sydney, NSW 2052, Australia. email: r.malaney@unsw.edu.au

processing time.²

Our adversary, Eve, is formidable - being fundamentally constrained only by the laws of physics. Most concerning for our QLV system is that Eve has at her disposal an unlimited number of colluding devices. Eve's internal communications can be classical and/or quantum, and are limited only by the non-signalling principle. I assume Eve can transmit secretly and directly through anything, knows the locations of all RSs at all times, and can intercept any signal sent by any RS. I also assume Eve's *finite* energy supply is limited only by the weak requirement that it is not detectable (e.g. via relativistic effects such as those influencing GPS timings [18]).

Gaussian States - For clarity, henceforth I will focus on the use of Gaussian CV quantum states (e.g. [20] for review) within the QLV system. In terms of the annihilation and creation operators \hat{a}, \hat{a}^\dagger , the quadrature operators \hat{q}, \hat{p} defined for photon states are ($\hbar = 2$ assumed) $\hat{q} = \hat{a} + \hat{a}^\dagger$ and $\hat{p} = i(\hat{a}^\dagger - \hat{a})$, satisfying $[\hat{q}, \hat{p}] = 2i$. The quadrature operators for a CV state with n modes can be defined by the vector $\hat{\mathbf{R}}_{1,\dots,n} = (\hat{q}_1, \hat{p}_1, \dots, \hat{q}_n, \hat{p}_n)$. Gaussian states are characterized solely by the first moments $\langle \hat{\mathbf{R}}_{1,\dots,n} \rangle$ and a covariance matrix \mathbf{M} , whose elements are given by $M_{ij} = \frac{1}{2} \langle \hat{R}_i \hat{R}_j + \hat{R}_j \hat{R}_i \rangle - \langle \hat{R}_i \rangle \langle \hat{R}_j \rangle$. \mathbf{M} can be transformed into $\mathbf{M}_s = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}$ where $\mathbf{A} = \tilde{a}\mathbf{I}_2$, $\mathbf{B} = \tilde{b}\mathbf{I}_2$, $\mathbf{C} = \text{diag}(c_+, c_-)$, $\tilde{a}, \tilde{b}, c_+, c_- \in \mathbb{R}$, and \mathbf{I}_2 is the 2×2 identity matrix. In this form the symplectic spectrum of the partially transposed covariance matrix is $\nu_\pm = ([\Delta \pm \sqrt{\Delta^2 - 4 \det \mathbf{M}_s}]/2)^{1/2}$, where $\Delta = \det \mathbf{A} + \det \mathbf{B} - 2 \det \mathbf{C}$. From the symplectic spectrum many fundamental properties of Gaussian states can be derived (see [20]). An important Gaussian state is the two-mode squeezed vacuum (TMSV) state, described for two modes a and b as $|s\rangle = \sqrt{1 - \lambda^2} \sum_{n=0}^{\infty} (-\lambda)^n |n\rangle_a |n\rangle_b$, where $\lambda = \tanh(r) \in [0, 1]$, and where $|n\rangle_a$ and $|n\rangle_b$ are Fock (number) states of modes a and b , respectively. Here, r is a parameter quantifying the two-mode squeezing operator $S_2(r) = \exp[r(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)]/2$. The covariance matrix for the TMSV state can then be written $\mathbf{M}_T = \begin{pmatrix} v\mathbf{I} & (\sqrt{v^2 - 1})\mathbf{Z} \\ (\sqrt{v^2 - 1})\mathbf{Z} & v\mathbf{I} \end{pmatrix}$ where the quadrature variance $v = \cosh(2r)$, and $\mathbf{Z} := \text{diag}(1, -1)$.

The TMSV state, being easily produced and manipulated, will likely play an important role in the Quantum Car. As well as being available for rounds of the QLV itself, the TMSV state could also be used as part of a quantum key distribution (QKD) process, in which a vehicle which has passed a location verification test is then allowed to set up secret keys between itself and other RSs. Indeed, the infrastructure and resources required for QKD in the vehicular setting are very similar to those required by QLV. Further, some of the messages transferred during rounds of both protocols can be 'double-dipped' upon. For example, classical information returned by

the PV could also be used as part of the error estimation phase of QKD. Combined QLV/QKD can be achieved directly via the use of some entangled states shared by the PV and RSs (or by the logically equivalent 'prepare and measure' schemes). Instruction on which states stored in memory are to be used for QKD can be sent as part of the QLV-VI request.

Decision Frameworks - Before discussing feasible threat models, let us first consider a generic formal decision framework based on some observation vector \mathbf{Y} . Our specific task within the context of the Quantum Car is to construct a binary-decision framework for determining whether claimed location information (e.g. a GPS report) delivered in the IEEE 1609.2 frames is to be trusted or not. If yes, the vehicle will retain (or be supplied with) a valid 1609.2 certificate; if no, the vehicle's existing certificates (if any) will be revoked (see [2]). The i th element of the vector \mathbf{Y} is of the form $Y_i = U_i + X_i$, with U_i being the value of a required metric estimated by (or from) an honest PV, and X_i being some unwanted noise. For a malicious PV I assume $Y_i = V_i + X_i$, with V_i being the value of a required metric being estimated by (or from) a malicious PV. In all models considered here I take X_i to be a zero-mean normal random variable with variance σ_i . Let $i = 1 \dots N$, N being the number of RSs participating in the measurement process at a given round (in some circumstances fewer RSs can be compensated for by more rounds). For simplicity, I assume $\sigma_i = \sigma$ for all i .

Let us consider two hypothesis, the null hypotheses \mathcal{H}_0 , and the alternate hypothesis \mathcal{H}_1 . Under \mathcal{H}_0 I assume the PV is legitimate, is at its claimed location (known by it exactly), and follows all coded instructions sent to it by the RSs in an honest and optimal fashion. Under \mathcal{H}_1 I assume the PV is malicious, holds as many devices as there are RSs participating in the measurement process, with none of those devices actually at the claimed location. Assuming the observations collected by different RSs are independent, under \mathcal{H}_0 the observation vector $\mathbf{Y} = [Y_1, \dots, Y_N]^T$ follows a multivariate normal distribution, $\mathbf{Y}|\mathcal{H}_0 \sim \mathcal{N}(\mathbf{U}, \mathbf{\Sigma})$, where $\mathbf{U} = [U_1, \dots, U_N]^T$ is a mean vector, and $\mathbf{\Sigma} = \sigma\mathbf{I}_N$. Under \mathcal{H}_1 we have $\mathbf{Y}|\mathcal{H}_1 \sim \mathcal{N}(\mathbf{V}, \mathbf{\Sigma})$, where $\mathbf{V} = [V_1, \dots, V_N]^T$ is a mean vector (note we have implicitly assumed the variance is the same under both hypothesis).

Assuming a likelihood ratio test, which is known to be optimal for a wide range of cost metrics within the realm of classical location verification frameworks [21–23], the following decision rule for our system (written as a ratio of likelihood

functions) can be constructed, $\Lambda(\mathbf{Y}) \triangleq \frac{p(\mathbf{Y}|\mathcal{H}_1)}{p(\mathbf{Y}|\mathcal{H}_0)} \stackrel{\mathcal{D}_1}{\underset{\mathcal{D}_0}{\gtrless}} \lambda$, where

λ is the threshold, and \mathcal{D}_0 and \mathcal{D}_1 are the binary decisions that infer whether the prover is legitimate or malicious, respectively. Given our assumption of Gaussian noise this can be re-written as $\mathbb{T}(\mathbf{Y}) \stackrel{\mathcal{D}_1}{\underset{\mathcal{D}_0}{\gtrless}} \Gamma$: $\mathbb{T}(\mathbf{Y}) \stackrel{\mathcal{D}_1}{\underset{\mathcal{D}_0}{\gtrless}} \Gamma$, where $\mathbb{T}(\mathbf{Y})$

is the test statistic given by $\mathbb{T}(\mathbf{Y}) \triangleq (\mathbf{V} - \mathbf{U})^T \mathbf{\Sigma}^{-1} \mathbf{Y}$, and Γ is a new threshold corresponding to $\mathbb{T}(\mathbf{Y})$ given by $\Gamma \triangleq \ln \lambda + \frac{1}{2} (\mathbf{V} - \mathbf{U})^T \mathbf{\Sigma}^{-1} (\mathbf{V} + \mathbf{U})$. Note, in this notation, the false positive rate and detection rates are $\alpha \triangleq \Pr(\mathbb{T}(\mathbf{Y}) \geq \Gamma | \mathcal{H}_0)$, $\beta \triangleq \Pr(\mathbb{T}(\mathbf{Y}) \geq \Gamma | \mathcal{H}_1)$, respectively.

²Processing time is fundamentally bound by the energy available to evolve between orthogonal states (see [19]). An adversary must have enough (undetectable) energy to ensure her additional combined processing time is undetectable. In the two feasible attacks studied here, I will assume enough energy is available to make all processing delays effectively zero.

Finally, a cost metric is chosen, as this will determine how to set the threshold λ (if the metric is optimized). A common choice for this is the total error $T_E = P_0\alpha + (1 - P_0)(1 - \beta)$, and I adopt that here with the *a priori* probability of legitimacy set at $P_0 = 1/2$. Having built our decision framework, let us now investigate a specific use of our generic QLV system.

In general, the PV does not know what operation(s) on what state(s) is needed at each round of the QLV until the full VI for that round is obtained. Faced with this, Eve can take two quite feasible approaches to attack the system. One is to wait until all the VI for that round is received, identify the CV state(s), determine which of her devices it is stored in, and then act on that state(s). The second is to try and copy the quantum information optimally beforehand, distributing copies to all devices, and act on those copies (as needed) as soon as the VI is fully received at each device. We refer to the first strategy as the *time-delay attack*, and the second strategy as the *optimal-cloning attack*. Our aim is to quantify the performance of the legitimate system against these two feasible attacks.

Let us consider the time-delay attack where a quadrature measurement is requested in a given round on a specific stored CV state - the result of which is broadcasted. In the attack, the classical output is delivered by Eve's devices to the required RSs - albeit at some vector of delays t_d (due to the time needed for Eve to communicate the measurement outcome to all devices). Using our previous relations we can determine the total error in the classification of the PV as a function of the verification distance and the number of observations N . The results of such a calculation are illustrated in Fig. 1a (left), which shows how the total error can be made arbitrarily small by increases in N . Similar trends to Fig. 1a can be found for other operations on the states.

In the optimal-cloning attack Eve utilizes a machine [24] that would copy a CV quantum state to multiple (one for each RS) optimal-fidelity clones [25]. In such an attack there is no time delay incurred (relative to an honest PV). However, any operational measurement on the cloned state(s) will lead to different statistics relative to the original state(s). For example, consider when the VI requests some stored CV states be sent to specific RSs (the legitimate system has the states needed for any comparison test). Fig. 1b (right) illustrates the case of a quadrature measurement operation used as a discriminating test in the scenario where the attack utilizes optimal clones derived from a single coherent state.³ Here I have used the general result that for $N_c \rightarrow M_c$ ($M_c \geq N_c$) cloning of N_c general coherent states, $M_c \geq 2$ being the number of equal fidelity optimal clones produced, the variance of the cloned states σ_{cl} will have an additional minimum variance $(2/N_c - 2/M_c)\sigma_0$, where σ_0 is the variance of the vacuum noise [25]. Discriminating between the different hypothesis in this circumstance takes a different form from a delay attack (the variance is no longer the same under both hypothesis). The test statistic for N observations (now the number of states tested) becomes $\sum_{i=1}^N (Y_i - U_i)^2$, and the threshold takes the

³The discrimination error by this (readily implementable) technique is greater than the Helstrom bound [27]. Quadrature measurements on other CV states (e.g. squeezed) can be optimal [28].

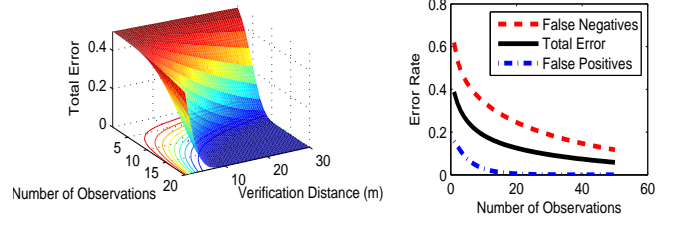


Fig. 1. (a) Total error (T_E) in QLV under a *time-delay attack* (color online). Here the RSs are all randomly positioned, $\lambda = 1$, and the standard deviation of the Gaussian noise in the timings is set at $1\mu s$. Eve has positioned her N devices optimally, each of them being some distance (the verification distance) from a claimed location. (b) T_E , the false negative rate ($1 - \beta$), and the false positive rate (α) as a function of the observation number (number of states tested), under an *optimal-cloning attack*. Here 5 optimal copies from 1 state are used, and λ is set so that $\Gamma = 2N$. Perfect quantum memory of the legitimate system is assumed, and timing information is assumed verified. The attacks (a) and (b) are the most feasible (simplest) from a classical and quantum perspective, respectively.

form $\Gamma = [(2\sigma_0\sigma_{cl}) / (\sigma_{cl} - \sigma_0)] [\log \lambda + N \log (\sigma_{cl}/\sigma_0)^{0.5}]$ (here the Y_i 's and U_i 's now refer to quadratures). Under these circumstances the false-positive rate is given by $1 - \chi_N^2(\Gamma/\sigma_0)$, where $\chi_N^2(x)$ is the chi-square cumulative distribution function with N degrees of freedom at the value x . Similarly, the detection rate is given by $1 - \chi_N^2(\Gamma/\sigma_{cl})$. Fig. 1b displays all the error rates for a specific parameter setting. Again, we can see that reduction of the total error with increasing N is once again possible - and that the total error can in principle be made arbitrarily small. Similar trends to Fig. 1b can be found for any cloning attack, including squeezed states and TMSV states (different tests may be used on the states).

Note, that I do not build into any \mathcal{H}_1 the possibility of a so-called teleportation attack [12]. Several issues can justify this. Arguably, the most important issue is a pragmatic one - the amount of resources needed for the attack in general appear unfeasible.⁴ In this work I simply adopt this view. However, I do also note, from an information-theoretic perspective, that in general the required teleportation needed for the attack is not available.⁵ For example, in CV-based QLV schemes the required CV teleportation (deterministic with unit fidelity) is not possible at finite energy.⁶ As such, it may be useful to

⁴The best bound on the number of entangled pairs needed for a successful teleportation attack (with unit fidelity obtained in the infinite port-number limit [26]) is of the form $2^{O(n)}$, where n is number of states to be teleported [13] (I remind the reader that $2^{270} \sim$ the number of nuclei in the observable universe). Pragmatism aside, an exponentially increasing amount of entanglement can eventually become detectable through its associated energy. Creation of any bipartite entanglement costs energy for temperatures $T > 0$ [32]. Reaching $T = 0$ requires infinite heat extraction.

⁵By this I mean with zero probability of detection using finite resources. That said, the attack of [12] poses a formidable in-principle challenge to QLV. For example, in the QLV of [7] 2^N N -bit messages are encoded in a non-orthogonal ensemble of stored entangled states, the ensemble being decoded later via classical inputs. Infinite resource issues aside, specific cases of [7] (e.g. dimension- N maximally-entangled qubit states with no null-signalling code component) are in-principle attackable by the *explicit* procedure given in [12]. Expanded expositions of the main concept in [12] are possible, but ultimately all energy requirements (e.g. teleportation, unitary evolution, erasures) must be bounded.

⁶Of course, realistic energy levels can push the CV teleportation fidelity arbitrary close to 1, but a non-unit fidelity is in-principle detectable (multiple rounds of teleportation at finite energy should enhance such detection).

look at the question posed by a teleportation attack from more of a *limited* legitimate-system viewpoint rather than from an attacker's *in-principle* viewpoint.⁷

Finally, I discuss how some quantum states can influence timing measurements made within the vehicular network. Assuming classical only signals, and Gaussian noise with variance σ_t in all the timing measurements, the variance ν_{cr} of the position error of a device located at (x_0, y_0) satisfies,

$$\nu_{cr}^{1/2} \geq c\sqrt{\sigma_t N} \left(\sum_{i=1}^{N-1} \sum_{j=i+1}^N \sin^2(\varphi_i - \varphi_j) \right)^{-1/2}, \text{ where the}$$

i th RS is at (x_i, y_i) , $\tan \varphi_i = (y_i - y_0) / (x_i - x_0)$ and c is the speed of light (e.g. [29, 30]). For some estimated position, we can see this leads to a $1/\sqrt{N}$ dependence for the location error. Implicit in the above bound is also a $1/\sqrt{N_p}$ dependence on the mean number of photons, N_p , used in each timing measurement. Quantum positioning [31] invokes the use of entangled states to shift this dependence to the form $1/N$, with squeezed states being used to provide a dependence of the form $1/N_p$. Fundamentally, both gains can be traced back to a higher spread in energy in the non-classical states, relative to coherent states. The resulting improved timings could be used to enhance the verification-decision process, or be used to simply enhance actual (or relative) position estimates of vehicles. For example, consider positioning via the use of laser signalling between vehicles. In this scenario, location errors in the *sub-mm* range can be anticipated using levels of entanglement and squeezing already achievable in the laboratory. Classical wireless positioning can sometimes lead us into the realm of the ‘dark arts’ (e.g. removal of biases, nuisance parameters [30]). The addition of quantum positioning techniques can only shed (non-classical) light.

Outlook - Our driverless vehicle 2.0 is certainly of the future - but not the *distant* future. The two main enablers needed - quantum memory of 1-day lifetime (or time between electric-quantum charges) and widespread vehicular communication infrastructure - appear within reach. Advances in quantum memory lifetimes are improving dramatically, with the current record (at a temperature of 2K) at 6 hours [33]. Confidence is high that photonic long-term quantum memory at *car-boot* temperature is achievable in the coming years [34]. Aside from the initial delivery of the quantum information (e.g. via optical fibre), QLV ‘in-the-field’ can operate with only classical wireless communication infrastructure - deployment of which in the wider vehicular context has already commenced. Of course, the driverless vehicle 3.0 will be even further advanced, deploying additional quantum technologies and applications.⁸ But 2.0 may keep our vehicle engineers busy, at least for now.

Conclusions - The quantum technologies discussed here will have many applications, offering unparalleled security and sensitivity in many scenarios. However, if the *number of lives saved* is the optimization metric of choice, use of these technologies in a widely-deployed vehicular network could

well deliver the *optimal* quantum-communication application.

- [1] G. Karagiannis *et al.*, Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions, IEEE Communications, Surveys and Tutorials, Vol. 13, No. 4, 2011.
- [2] T. Zhang, L. Delgrossi, Vehicle safety communications, Wiley, 2012.
- [3] A. Broggi *et al.*, Public road urban driverless-car test, IEEE Trans. Intelligent Transportation Systems, Vol. 16, No. 6, 2015.
- [4] J. T. Chiang, J. J. Haas, J. Choi, Y. Hu, Secure location verification using simultaneous multilateration, IEEE Trans. Wireless Commun., vol. 11, no. 2, pp. 584-591, 2012.
- [5] N. Chandran, V. Goyal, R. Moriarty, R. Ostrovsky, Position based cryptography, SIAM J. Comput., 43(4), pp. 1291-1341, 2014.
- [6] W. Wootters, W. Zurek, A single quantum cannot be cloned, Nature 299, pp. 802-803, 1982. (Also, D. Dieks, Phys. Lett. A, 92 (6), 271, 1982).
- [7] R. Malaney, Location-dependent communications using quantum entanglement (arXiv:1003.0949) Phys. Rev. A 81, 042319, 2010.
- [8] R. Malaney, Quantum location verification in noisy channels (arXiv:1004.4689), IEEE Globecom 2010, pp. 1-6, 2010.
- [9] N. Chandran *et al.*, arXiv:1005.1750 (replaced by [12]), 2010.
- [10] A. Kent, W. Munro, T. Spiller, Quantum tagging: authenticating location via quantum information and relativistic signalling constraints (arXiv:1008.2147), Phys. Rev., A 84, 012326, 2011.
- [11] H.-K. Lau, H.-K. Lo, Insecurity of position-based quantum-cryptography protocols against entanglement attacks (arXiv:1009.2256), Phys. Rev. A 83: 012322, 2011.
- [12] H. Buhrman *et al.*, Position-based quantum cryptography: impossibility and constructions, Advances in Cryptology (arXiv:1009.2490), Lecture Notes in Computer Science, Vol. 6841, pp. 429-446, 2011.
- [13] S. Beigi, R. König, Simplified instantaneous non-local quantum computation with applications to position-based cryptography (arXiv:1101.1065), New Journal of Physics, 13, 093036, 2011.
- [14] M. Nadeem, Position-based quantum cryptography over untrusted networks, Laser Phys. 24, 085202, 2014.
- [15] K. Chakraborty, A. Leverrier, Practical position-based quantum cryptography, Phys. Rev. A 92, 052304, 2015.
- [16] A. Kent, R. Beausoleil, W. Munro, T. Spiller, Tagging systems, US Patent US7075438, 2006.
- [17] A. Kent, private communication, August 2010.
- [18] N. Ashby, Relativity in the GPS, Living Rev. Relativity, 6, 1, 2003.
- [19] L. B. Levitin, T. Toffoli, Fundamental limit on the rate of quantum dynamics, Phys. Rev. Lett. 103, 160502, 2009.
- [20] C. Weedbrook, *et al.*, Gaussian quantum information, Reviews of Modern Physics, 84, pp. 621 - 669, 2012.
- [21] S. Yan, R. Malaney, I. Nevat, G. W. Peters, Optimal information-theoretic wireless location verification, IEEE Trans. on Vehicular Technology, Vol. 63, Issue 7, pp. 3410-3422, 2014.
- [22] S. Yan, R. Malaney, I. Nevat, G. W. Peters, Timing information in wireless communications and optimal location verification frameworks, AusCTW, doi:10.1109/AusCTW.2014.6766443, 2014.
- [23] S. Yan, R. Malaney, I. Nevat, G. W. Peters, Location verification systems for VANETs in Rician fading channels, IEEE Trans. on Vehicular Technology, (doi: 10.1109/TVT.2015.2453160) 2015.
- [24] V. Bužek, M. Hillery, Quantum copying: Beyond the no-cloning theorem, Phys. Rev. A 54, 1844, 1996.
- [25] N. J. Cerf, S. Iblisdir, Optimal N-to-M cloning of conjugate quantum variables, Phys. Rev. A 62, 040301(R), 2000. (Also, G. Lindblad, J. Phys. A 33, 5059, 2000.)
- [26] S. Ishizaka, T. Hiroshima, Quantum teleportation scheme by selecting one of multiple output ports, Phys. Rev. A 79, 042306, 2009.
- [27] C. W. Helstrom, Quantum detection and estimation theory, Mathematics in Science and Engineering, Vol. 123, 1976.
- [28] H. Nha, H. J. Carmichael, Distinguishing two single-mode Gaussian states by homodyne detection: An information-theoretic approach, Phys. Rev. A 71, 032336, 2005.
- [29] N. Patwari, *et al.*, Relative location estimation in wireless sensor networks, IEEE Trans. Signal Proc., vol. 51, no. 8, pp. 2137-2148, 2003.
- [30] R. Malaney, Nuisance Parameters and location accuracy in log-normal fading models, IEEE Trans. Wireless Commun., Vol. 6 pp. 937-947, 2007.
- [31] V. Giovannetti, S. Lloyd, L. Maccone, Quantum enhanced positioning and clock synchronization, Nature, 412, 417, 2001.
- [32] M. Huber, *et al.*, Thermodynamic cost of creating correlations, New J. Phys. 17, 065008, 2015.
- [33] M. Zhong *et al.*, Optically addressable nuclear spins in a solid with a six-hour coherence time, Nature 517, 177180, 2015.
- [34] K. Heshamia, *et al.*, Quantum memories: emerging applications and recent advances (arXiv:1511.04018), 2015.

⁷E.g. - For some $0 < \epsilon < 1$, under what restrictions on the operations of a legitimate system, can an adversary using some defined finite resource produce an undetectable attack with a success probability $1 - \epsilon$?

⁸For example, entanglement (perhaps macroscopic) shared between vehicles for enhanced inter-vehicle control and network synchronization.